Processing and Access of Critical or Sensitive information (Before collection)

Description

Active Mail has guidelines for all employees regarding the Processing and Access of Critical or Sensitive information (Before collection).

Purpose & Scope

The purpose of this policy is to explain the general procedures relating to the Processing and Access of Critical or Sensitive information (Before collection).

The following guidelines are to be adhered to by all employers, supervisors and employees.

Policy & Procedure

All employees are required to adhere to the below polices when processing, gathering or inputting client/customer data into Active Mail's environment.

Obtaining consent:

At the point of data collection (whether that be in the contact forms, by other means) customers will be provided with the required information such as our User Agreement at this point of collection (or closest instance possible to point of collection, such as providing via email to phone orders) to ensure that the customer is fully aware of their rights in regards to this data and also what the use of this data will be.

Collection of personal data:

Active Mail will, from time to time, receive and store personal information you enter onto our website, provided to us directly or given to us in other forms.

You may provide basic information such as your name, phone number, address and email address to enable us to send information, provide updates and process your product or service order. We may collect additional information at other times, including but not limited to, when you provide feedback, when you provide information about your personal or business affairs, change your content or email preference, respond to surveys and/or promotions, provide financial or credit card information, or communicate with our customer support.

Additionally, we may also collect any other information you provide while interacting with us.

How we collect data:

Active Mail collects personal information from you in a variety of ways, including when you interact with us electronically or in person, when you access our website and when we provide our services to you. We may receive personal information from third parties. If we do, we will protect it as set out in this Privacy Policy.

Use of personal data:

Active Mail may use personal information collected from you to provide you with information, updates and our services. We may also make you aware of new and additional products, services and opportunities available to you. We may use your personal information to improve our products and services and better understand your needs.

Active Mail may contact you by a variety of measures including, but not limited to telephone, email or mail.

Withdrawal of consent:

Active Mail appreciates that individuals or business' may require or request for their information to be removed from our systems. We ensure your details are suppressed in our systems to ensure you are not contacted in the future.

There may be instances where a customer will request for their data to be removed, however, we may be unable to action this request immediately due to previously contracted work/services. In an instance such as this we will contact the customer directly via phone or email and devise a strategy to ensure the best possible outcome for the customer. This will be dictated on a case by case basis and will require approval from senior management.

Disclosure of your personal information

We may disclose your personal information to any of our employees or IT contractor insofar as reasonably necessary for the purposes set out in this Policy, Personal information is only supplied to a third party when it is required for the delivery of our services.

We may from time to time need to disclose personal information to comply with a legal requirement, such as a law, regulation, court order, subpoena, warrant, in the course of a legal proceeding or in response to a law enforcement agency request.

We may also use your personal information to protect the copyright, trademarks, legal rights, property or safety of Active Mail, activemail.com.au, its customers or third parties.

If there is a change of control in our business or a sale or transfer of business assets, we reserve the right to transfer to the extent permissible at law our user databases, together with any personal information and non-personal information contained in those databases. This information may be disclosed to a potential purchaser under an agreement to maintain confidentiality. We would seek to only disclose information in good faith and where required by any of the above circumstances.

By providing us with personal information, you consent to the terms of this Privacy Policy and the types of disclosure covered by this Policy. Where we disclose your personal information to third parties, we will request that the third party follow this Policy regarding handling your personal information.

Security of your personal information

Active Mail is committed to ensuring that the information you provide to us is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure information and protect it from misuse, interference, loss and unauthorised access, modification and disclosure.

The transmission and exchange of information is carried out at your own risk. We cannot guarantee the security of any information that you transmit to us, or receive from us. Although we take measures to safeguard against unauthorised disclosures of information, we cannot assure you that personal information that we collect will not be disclosed in a manner that is inconsistent with this Privacy Policy.

Changes to Privacy Policy

This Privacy Policy in the future. We may modify this Policy at any time, in our sole discretion and all modifications will be effective immediately upon our posting of the modifications on our website or notice board. Please check back from time to time to review our Privacy Policy.

Website

When you visit our website (activemail.com.au) we may collect certain information such as browser type, operating system, website visited immediately Internal Document – Privacy Policy before coming to our site,

etc. This information is used in an aggregated manner to analyse how people use our site, such that we can improve our service.

Cookies

We may from time to time use cookies on our website. Cookies are very small files which a website uses to identify you when you come back to the site and to store details about your use of the site. Cookies are not malicious programs that access or damage your computer. Most web browsers automatically accept cookies but you can choose to reject cookies by changing your browser settings.

Processing and access of Critical or sensitive Information (After Collection)

Description

Active Mail has guidelines for all employees regarding the Processing and Access of Critical or Sensitive information (after collection).

Purpose & Scope

The purpose of this policy is to explain the general procedures relating to the processing and access of critical or sensitive information (after collection).

The following guidelines are to be adhered to by all employers, supervisors, and employees.

Policy & Procedure

As part of our operations, we need to obtain and process information. This information includes any data that makes a person or company identifiable such as names, addresses, business information.
Active Mail collects this information in a secure way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

2. All data and information will be managed and stored within the Active Mail secure network and stored on our inhouse servers. No information is to be stored in cloud solutions or with third party storage providers.
3. All information is to be accurate and kept up to date
4. Received securely and for lawful business purposes
5. Processed by the company within its legal and moral boundaries
6. Protected against any unauthorised or illegal access by internal or external parties.
7. It will not be:
    a. Communicated informally,
    b. Stored for more than a specified amount of time
    c. Transferred to organisations, states, or countries
    d. Distributed to any party other than the ones agreed upon by the data's owner

8. In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs. Specifically, we must:
    a. Inform people about how we'll process their data
    b. Inform people about who has access to their information
    c. Have provisions in cases of lost, corrupted, or compromised data

In addition to the above, Critical and sensitive information will be physically & technologically protected from unauthorised access, damage and interference as per the policies of the externally contracted bodies or Active Mail practices where appropriate.

Access to all information will be controlled via a hierarchical admin system, where no alteration to the hardware configuration of the system may take place without the permission of the MD.

As per the above, all access outside of the MD will be driven by business requirements. Access can be granted or arrangements made on either a temporary or permanent basis for employees, partners, suppliers according to their role, only to a level that will allow them to carry out their duties. Furthermore, where possible Multi Factor Authentication (MFA) will be utilized by Active Mail Staff to access sensitive environments such as the production environment on our software platform.

Data is categorised according to the protection it needs, as derived from the risk analysis or assessment of the head of Development. The following categories have been identified (presented in order of increasing sensitivity. Also described within the "Information Classification Scheme"):

- **Public**: information and data that can be disclosed.

- **Confidential**: information and data that is subject to legislation on protection of personal data. Disclosure of this data requires specific permission / license.
- **Restricted**: information and data that is important for seamless operation and should be subject to strict controls and protected.

The requirements of information security and the way data is processed vary according to the category of information. All employees are trained on security protocols and data protection.

Regarding individual and employee access, all partners, staff and relevant parties will be provided with individual login credentials, with the ability for a user to amend their password at any time they may feel compromised or otherwise in jeopardy. Actions can also be attributed to a specific user due to this system. This applies to the operating system level and application level.

The requirements for login credentials are as follows:

- Each user has a unique identity (user ID).
- A list of users and their unique identities is maintained.
- Each authentication identifier is assigned to a user and is used by a single user.
- The system administrators have identities that correspond to accounts with elevated privileges.

When generating a password, it is recommended that a combination of alphabetic, numeric, upper and lower case and system characters be used. Furthermore, Passwords should not be written down except as possible reference by Bethany IT under strict security control. Passwords are not to be revealed to or shared with other users.

Logical access control is achieved via a process of a formal user registration and de- registration procedure, which provides a means for granting and revoking access to all information and services, specifically:

- Registered user accounts are reviewed for applicability at specific periods. (annually)
- Privileges are defined for specific business purposes.
- The allocation and use of privileges is restricted and controlled.
- Privileges and privilege allocation is reviewed for applicability at specified periods.
- The allocation and establishment of user passwords is controlled through a formal management process.
- Users are required to follow good security practices in the selection use of passwords as outlined in this policy

Our team will make every effort to review the data collected within our CRM on a regular basis to ensure that not only the permissions are still relevant, and the data contained within. These audits occur on a recurring basis with the intervals set depending on the nature of the data. I.e., The information collected by our CRM from our contact forms, checkout and other means will be reviewed monthly to ensure that there are no duplicates or errors in recently collected data.

In addition to this, upon request, we will work to provide the customer with all the information Active Mail has stored within our CRM. This will be provided via a variety of means varying on the stored information (exports where available, otherwise via screenshots or direct access to review, or any other relevant means). Furthermore, should any errors exist in the data we have retained due to any reason, Active Mail will make every effort to ensure that this data is corrected. While the most opportune instance for this to occur is during a customer's elective data review, we understand that this may not occur on a regular basis. At the relevant points of recollection our team will ensure that details such as the following are updated:

- Customer contact details such as email and contact number – Will be reviewed during our teams ongoing & regular (approximately every 3 months) interactions
- Customer address and payment details – Will be updated and reviewed on a regular basis.

The intention of this policy, its stipulations and all adjoining Active Mail Policies is to protect all user/personal data throughout its lifecycle while providing transparency to Active Mail's greater client base. This includes but is not limited to the assurance that data will not be accessed by Active Mail /a third party or used by Active Mail /a third party in any manner which is not explicitly stated by the owner of said data. Active Mail is committed to implementation of policies and practices which ensure all data within our systems is kept private, with multiple systems in place ensuring that the best possible practices are adhered to. This multi system approach to data privacy & security is a facilitated on a "By Design" level. These systems are intended to be complementary to one another to ensure overlap is achieved, and no gaps are present within the greater Active Mail ecosystem.